Lettre à Mme Hamer*

by Jean-Pierre Serre

COLLÈGE
DE
FRANCE
—
3. rue d'Ulm
75321 Paris Cedex 05

Chère Madame,

Je vais vous raconter ce qu'il est advenu de votre congruence sur les polynômes de Chebyshev:

Tate m'a écrit (e-mail) en avril qu'il venait de retrouver dans ses papiers un texte de vous, vieux de 2 ans, où vous démontriez une certaine congruence sur les polynômes "Y_k" (votre notation), au moyen de formes modulaires mod p, et où vous posiez la question d'en trouver une démonstration directe. Il me demandait ce que j'en pensais. J'ai commencé par fabriquer une telle démonstration. Voici comment: si l'on écrit y sous la forme $y = t + 2 + t^{-1}$, on a $Y_k(y) = \left(1 + t + \ldots + t^k\right)/t^{k/2}$ (k est pair, d'après vos conventions). Bien sûr, cela est aussi vrai (mod p), à condition de prendre t dans le corps $\mathbb{F}_{p^2}$. D'où deux cas à distinguer:

a) On a $t \in \mathbb{F}_p$, i.e. $t^p = t$, et si $t \neq 1$, on a $1 + t + \ldots + t^{p-2} = 0$, d'où, si $k' = k - (p-1)$:

$$Y_{k'}(y) = Y_k(y) \cdot \left(\frac{t}{p}\right).$$

Mais on a $\left(\frac{t}{p}\right) = \left(\frac{y}{p}\right)$ (car $yt = (t+1)^2$). On peut donc écrire la congruence ci-dessus sous la forme $Y_{k'}(y) = \left(\frac{y}{p}\right) \cdot Y_k(y)$. Du coup, dans votre formule à 4 termes :

$$A - B - C - D \stackrel{?}{=} 0,$$

on a $A = B$ et $C = D$, de sorte que la formule est bien vraie.

b) Lorsque t n'appartient pas à $\mathbb{F}_p$, on a $t^p = 1/t$, d'où

$$1 + t + \ldots + t^p = 0$$

et si l'on pose cette fois $k'' = k - p - 1$, on trouve comme ci-dessus

$$Y_{k''}(y) = t^{(p+1)/2} Y_k(y) = \left(\frac{y}{p}\right) \cdot Y_k(y) = \left(\frac{y}{p}\right) \cdot Y_k(y).$$

(Il faut faire un petit calcul pour voir que $\left(\frac{y}{p}\right)$ est égal à $t^{(p+1)/2}$.) D'où:

$$Y_{k''}(y) = \left(\frac{y}{p}\right) \cdot Y_k(y),$$

*This is a LaTeX version of Jean-Pierre Serre's letter on July 2, 2001 to Carol Hamer, typeset by Haoran Liang. All errors are mine.

ce qui donne $A = C$, et $B = D$, et votre formule $A - B - C + D = 0$ est donc démontrée dans tous les cas.

Cette vérification "à la main" ne m'a pas beaucoup plu. Il y a diverses restrictions peu naturelles, par exemple k pair, ou $p > 3$. En outre, je suis habitué à voir les polynômes de Chebyshev comme les *traces* de représentations de groupes. J'ai donc cherché à expliciter l'énoncé de théorie des groupes suggéré par votre congruence. Voici ce que ça a donné:

Soit F un corps fini à q éléments, et soit G le groupe $\mathrm{GL}_2(F)$. Soit V la représentation naturelle de degré 2 de G (sur le corps F). Pour tout entier $k \geqq 0$, soit $V(k) = \mathrm{Sym}^k V$ la puissance symétrique k-ième de V. Soit $e\colon G \to F^\times = \mathrm{GL}_1(F)$ le caractère "déterminant", i.e. $e = \wedge^2 V$. Enfin, soit $K(G) = K(G, F)$ le groupe de Grothendieck des $F[G]$-modules de dimension finie. On peut regarder les $V(k)$, ainsi que e, comme des éléments de l'anneau $K(G)$. Dans cet anneau, $e.V(k)$ correspond au produit tensoriel de $V(k)$ par e (c'est un "Tate twist", si 1'on veut...).

Théorème 1 *Si $k \geqslant 2q$, on a $V(k) - V(k-q+1) - e.V(k-q-1) + e.V(k-2q) = 0$ dans $K(G)$.*

(Pour retrouver votre formule à partir de là, il faut prendre $q = p$, k pair, et remarquer que toute égalité dans $K(G)$ entraîne une égalité analogue pour les traces.)

La démonstration du théorème ne fait pas de difficultés: d'après Brauer, il suffit de vérifier l'égalité correspondante pour les caractères modulaires des représentations $V(k)$, $V(k-q+1)$, etc. Or ces caractères sont faciles à calculer. Les éléments p-réguliers de G sont de deux sortes: ceux dont les valeurs propres appartiennent à F, et ceux dont les valeurs propres sont conjuguées sur F par $z \mapsto z^q$. On trouve ainsi:

a) Si $g \in G$ appartient au centre de G (i.e. si c'est une homothétie de rapport $z \in F^\times$), les caractères de $V(k)$, ... en g sont égaux au produit de z^k par $(k+1)$, $(k-q+2)$, $(k-q)$, $(k-2q+1)$ et l'on a bien:

$$k + 1 - (k - q + 2) - (k - q) + k - 2q + 1 = 0.$$

b) Si les valeurs propres de g appartiennent à $\mathbb{F}$ et sont distinctes, le même calcul qu'à la lère page montre que les caractères de $V(k)$ et de $V(k-q+1)$ sont égaux en g; même chose pour $V(k-q-1)$ et $V(k-2q)$. D'où l'égalité cherchée, d'après le schéma "$A = B$" et "$C = D$" $\Rightarrow A - B - C + D = 0$.

c) Calcul analogue dans le cas restant, celui de deux valeurs propres conjuguées sur le corps F. Ici le schéma est "$A = C$" et "$B = D$" $\Rightarrow A - B - C + D = 0$.

Il y a une chose un peu déplaisante dans ce théorème, c'est la restriction $k \geqslant 2q$, qui apparaît pour que l' on puisse donner un sens à $V(k-2q)$. On peut s'en débarrasser de la façon suivante: on prolonge la définition de $V(k)$ aux entiers $k < 0$ en posant:

$$V(-k) = -e^{1-k} V(k-2), \quad \text{pour tout } k \in \mathbb{Z}, \tag{D}$$

ce qui a un sens dans le groupe de Grothendieck $K(G)$ (on convient aussi que $V(-1) = 0$).

Avec cette convention (qui est suggérée par l'expression du caractère modulaire de Brauer), on constate que le théorème de la p.2 est vrai pour tout $k \in \mathbb{Z}$. Même calcul!

(Exemple: si l'on prend $k = q$, on a $V(k-q+1) = V(1)$, $V(k-q-1) = V(-1) = 0$ et $V(k-2q) = V(-q) = -e^{1-q} V(q-2) = -V(q-2)$, d'où l'égalité:

$$V(q) = V(1) + e.V(q-2),$$

ce qui est facile à vérifier directement.)

Ce jeu ne s'arrête pas là. Il est naturel de se demander si l'égalité du théorème de la p.2, qui concerne seulement des éléments de $K(G)$, ne dissimule pas quelque chose de plus précis, à savoir un isomorphisme entre G-modules (alors que $K(G)$ ne s'occupe que des semi-simplifiés). C'est bien le cas, au moins en partie. Bornons-nous aux entiers $k > q$, de sorte que l'entier $k'' = k - (q+1)$ soit $\geqq 0$. La version "module" du théorème est la suivante:

Théorème 2 *Il existe une suite exacte de $F[G]$-modules :*

$$0 \to e.V(k-q-1) \to V(k) \to S(k) \to 0,$$

où $S(k)$ est un module qui ne dépend que de la classe de k modulo $q-1$.

(En appliquant ceci à k et $k-(p-1)$, on obtient un isomorphisme :

$$V(k)/e.V(k-q-1) \simeq V(k-q+1)/e.V(k-2q) \quad (\text{si } k \geqq 2q),$$

ce qui redonne le théorème de la p.2.)

Voici le principe de la démonstration. On choisit une base (x,y) de V, ce qui donne une base $(x^k, x^{k-1}y, \ldots, y^k)$ de chacun des $V(k)$. Soit P l'élément de $V(q+1)$ défini par $P = xq^y - xy^q$ (P est un"invariant de Dickson", cf. Bourbaki, LIE V, p.138). Cet élément de $V(p)$ est presque invariant par G: si $g \in G$, on a $g.P = e(g).P$. Il en résulte que la multiplication par P est un homomorphisme (évidemment injectif) de $e.V(k-q-1)$ dans $V(k)$. Le conoyau n'est pas difficile à déterminer: on trouve que c'est le module $\mathrm{Ind}_B^G\left(\chi^k\right)$, où B est le Borel de G formé des $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ et χ est le caractère de B donné par $\chi\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\right) = a^k$. D'où le théorème.

Il y a une autre façon de voir tout ceci, en termes de géométrie algébrique. Si X désigne la droite projective $\mathbb{P}_1$ sur le corps F, on peut munir X de son faisceau bien connu "$\mathcal{O}(k)$" (pour $k \in \mathbb{Z}$); le groupe G opère de façon naturelle sur X et aussi sur (k). D'où une action sur les groupes de cohomologie $\mathrm{H}^i(X, \mathcal{O}(k))$ pour $i = 0, 1$ (les autres sont nuls). On peut donc définir un élément de $K(G)$ en posant à la manière habituelle :

$$\mathrm{EP}(k) = \mathrm{H}^0(X, \mathcal{O}(k)) - \mathrm{H}^1(X, \mathcal{O}(k)).$$

Si $k \geqq 0$, le H^1 est nul, et l'on a donc $\mathrm{EP}(k) = \mathrm{H}^0(X, \mathcal{O}(k)) = V(k)$. Si $k < 0$, c'est le H^0 qui est 0, et le "théorème de dualité" permet de déterminer $\mathrm{H}^1(X, \mathcal{O}(k))$ en termes de $\mathrm{H}^0(X, \mathcal{O}(2-k))$. Vu la formule (D) de la p.3, on voit donc que la somme alternée $\mathrm{EP}(k)$ est égale à $V(k)$ pour tout $k \in \mathbb{Z}$, ce qui explique les formules.

Quant à la démonstration de la page précédente, basée sur le polynôme P, elle s'interprète très bien en termes de faisceaux; comme les zéros de P sont les points F-rationnels de $X = \mathbb{P}_1$, on voit ce qu'est $S(k)$: c'est simplement le produit des fibres de $\mathcal{O}(k)$ aux différents points de $\mathbb{P}_1(F)$.

J'en suis là. Bien sûr, j'aimerais savoir ce qui se passe pour d'autres groupes que GL_2, par exemple GL_n (pour lequel il y a aussi des polynômes de Dickson) ou même des groupes réductifs plus ou moins quelconques. Une formule comme la formule de dualité (D) de la p.3 est bien connue (pour des groupes réductifs quelconques): J.C. Jantzen, Repr. of Algebraic Groups, p.303.

Pour revenir aux formes modulaires: Oesterlé a un étudiant qui travaille sur les formes modulaires mod p, via la théorie des "symboles". Or la théorie des symboles est un jeu qui se passe à peu près entièrement à l'intérieur du groupe $\mathrm{GL}_2\left(\mathbb{F}_p\right)$ - c'est du moins ce qu'Oesterlé m'a dit. On peut donc appliquer les énoncés de la présente lettre aux formes modulaires mod p: on revient ainsi à votre point de départ!

Bien à vous - et toutes mes excuses pour avoir été un peu trop long...

J.-P. Serre
6 avenue de Montespan
75116 PARIS